higordiego / **VULN-003-idor-cross-tenant-invoice-access.md** Secret

Created 3 weeks ago

Code Revisions 1

VULN-003-idor-cross-tenant-invoice-access.md

Affected Version:

- **Invoice System in Laravel**: 1.0

Vulnerability Information:

- **Vulnerability Type:** IDOR + Cross-Tenant Data Exposure
- **Severity:** CRITICAL
- **Status:** Unpatched

Vulnerable Endpoint:

- `/invoice/{id}` (GET/PUT methods)

Vulnerability Description:

Invoice records are accessed by raw ID without validating that the record belongs to the requesting company (tenant). While the index view is scoped, direct access to a specific invoice allows an attacker to view or edit invoices from any other company in the system.

Proof of Concept (PoC):

Below is a **GET** request demonstrating unauthorized cross-tenant invoice access:

```
GET /invoice/5 HTTP/1.1
Host: localhost
```

Explanation:

The attack relies on direct enumeration:

```
id=5
```

By providing an invoice ID belonging to another company, the attacker bypasses tenant isolation because the controller lacks a `company_id` check.

Impact:

- **Confidentiality:** Exposure of sensitive billing and financial data belonging to other companies.
- **Integrity:** Unauthorized modification of invoices, amounts, and statuses.
- **Business Risk:** Disclosure of customer lists and transaction history across the platform.

Mitigation Recommendations:

1. **Scope Queries:** Always include a tenant check in queries: `Invoice::where('company_id', auth()->user()->company_id)->findOrFail($id)`.
2. **Use Policies:** Apply Laravel Policies to every read/write action on the Invoice model.
3. **Route Model Binding:** Use scoped bindings to automatically enforce tenant isolation.